EMERGING PRIVACY ISSUES

Willis H. Ware

October 1985

P-7145

The Rand Paper Series

Papers are issued by The Rand Corporation as a service to its professional staff. Their purpose is to facilitate the exchange of ideas among those who share the author's research interests; Papers are not reports prepared in fulfillment of Rand's contracts or grants. Views expressed in a Paper are the author's own and are not necessarily shared by Rand or its research sponsors.

The Rand Corporation, 1700 Main Street, P.O. Box 2138, Santa Monica, CA 90406-2138

EMERGING PRIVACY ISSUES*

INTRODUCTION

I want to speak broadly about privacy issues this morning. I would like to suggest new aspects of it and also to try out some ideas because there are themes not now in the public debate that I believe must be surfaced. Certainly I must relate privacy concerns to security as we will face it ahead and to any law that we may wish to create. Of necessity, I will present the discussion in the United States context; I do not know the European situation well enough, especially to illustrate points from time to time.

I do want to treat this presentation in the nature of a conference keynote. I will try to suggest things that the conference might wish to talk about; hopefully, I can plant seeds in the minds of conferees. But I will raise more issues and questions than I can provide answers.

Privacy Now

First of all, what is privacy as we know it in our professional world of informatics? Historically, it has dealt with information about people, and the way such information is used to make decisions about them, primarily in regard to a determination of entitlements, rights, or privileges a given person might have. As such, the thrust of privacy concern has been to assure that such information is accurate and complete for the intended use, and that its use would be confined to that intended at the time the information was provided by the individual to the record keeper. The issue as it has developed over the last 15 years is sometimes called information privacy or record-keeping privacy.

In the United States the first records of concern were those related to personal credit. As other law has been implemented, there have of course been many compromises between the strict ideal situation and practical reality. For example, United States law is generally easy

---

*Presented as keynote speech at IFIP/SEC'85, Trinity College, Dublin, Ireland, August 13, 1985. To be published in the conference proceedings by North-Holland Publishing Company, Amsterdam.

to circumvent with regard to the intended use of information, or "routine use" as it is called in the 1974 Privacy Act. Federal agencies find it quite simple to use information initially collected for one purpose for some other purposes later.

The thrust of United States privacy law has been predominantly to assure the proper use of information by authorized users; organizations who hold information are responsible for assuring that it is used for its intended use and for assuring its accuracy. In general, the protection is that of a "Code of Fair Information Practices," the details of which were conceived in early 1973 and presented to government officials in July of the same year. The law has given only minor attention to the risk of information falling into unauthorized hands as a result of system penetrations or compromises, malfunctions, design flaws, or poor operating procedures. It does not address the possibility that information will be pilfered from systems and used to the disservice of an individual.

Regrettably, computer security is only addressed indirectly in United States law; agencies are simply directed to protect information but the threat against information is not even specified. United States law does, through its routine use provisions, concern itself with the improper transfer of information from one record keeper to another; such a transfer would be a form of use by unauthorized recipients.

The law is quite different, of course, in other countries not only in the details of protection afforded individuals but in regard to implementation of the law and its ongoing oversight. For example, in Europe the general arrangement is a Data Protection Board or an entity of similar name; there is usually a federal official in charge of the situation. A record system often must apply for permission to exist, and there is an agreed upon set of rules governing its behavior. The Board often is a body through which an individual can seek remedial action against the record keeper. In the United States, there is only loose oversight by the Office of Management and Budget supplemented by an annual report to the Congress about how the law has worked in the past year; there is no official in overall charge of privacy.

A United States citizen must be prepared to take a lot of after-the-fact action to protect his rights. There is a real minimum of a priori protection assured to him, but he is helped somewhat by consumer protection agencies which play some role in supporting the individual. Basically, he is on his own most of the time.

Privacy Ahead

Privacy ahead will have additional dimensions. It will retain its record-keeping aspect; but much information will be collected, explicitly or otherwise, about individuals that is not intended for decisionmaking in the usual sense and could be used to harm or to put an individual or group at a disadvantage. But as I hope to show you in this discussion, privacy in the years ahead will be much more complex than the relatively straightforward issues that have been faced in record keeping--complexity in terms of the number of organizations involved, in terms of the intricacy of the information flows, and in terms of the difficulty of conceiving appropriate legal safeguards. It is not at all certain that the practices and law which have been developed for present privacy protection can work for new situations.

EXPECTATIONS

I would like to suggest several basic attributes of the privacy situation, as I see it developing. In a sense, they can form a framework for identifying potential privacy invasions and infractions.

Over calendar time, perhaps over a lifetime or even more than one generation, people build up expectations about the behavior of the environment in which they are immersed, and with which they must interact. So to speak, people come to understand how something--like the banking system--works and derive a set of expectations about how it will respond to an action by an individual. They also learn how to exploit its characteristics for personal advantage and to utilize anomalies that might exist, e.g., to use the cash float for personal funds managment. This is especially true of record-keeping or communication systems, which can be seen simply as the technological embodiments of the basic information processes that make one's personal life, society, government, and all of commerce and industry function.

Often the expectations transcend simple operational details and include protections of information that an individual perceives as important to himself, or that society and its processes have deemed important for the overall good. Such broader expectations arise from past experiences with systems and organizations, from specific instances of system behavior, from the legislative framework, from administrative rulings, or even from judicial processes and case law decisions. Moreover, the totality of one's expectations stem not only from his own life experience but also from the many decades of past history.

However, information technology has, in recent years, maintained a very rapid rate of progress with the consequence that computer and communication-based information systems have proliferated rapidly, introduced many new consumer services and products, many new uses of information and new information services. Such systems have pervaded societal institutions--government, industry, education, transportation, entertainment, travel, medicine, health care delivery, etc. In some, possibly many, instances the onrush of technology has abruptly changed the actual workings of systems and organizations, often invisibly to the individual. Commonly, laws fail to keep up with technology changes or are easily end-run or circumvented.

As one might expect, people will carry their expectations forward to the new environment, not realizing that some or all of them may no longer be valid or may have even been destroyed completely. People can therefore be at risk in new ways not foreseen or lose some right, privilege, or legal standing but not know it. Let me offer some examples.

Electronic Mail

Historically, individual or business correspondence has been assured that it will have the protection of a sealed envelope from sender to recipient. Such protection has been written into law, and the exceptions to it were carefully stipulated and controlled. For example, a legal process must take place before a sealed envelope can be opened although the so-called mail cover is easier to implement. Moreover, we implicitly pay for the protection through the additional cost of first-

class service that allows an envelope to be sealed. International agreements have also existed to extend sealed-envelope protection across national borders.

Electronic mail does not provide end-to-end protection of similar nature. From the time a sender creates a message, either at his own electronic terminal or by delivering it to a commercial service, until it is seen by the recipient, the material is in electronic forms that are readily interceptable and readable by anyone with the necessary equipment. Thus, the casual extrapolation of experiences based on the traditional mail system to an electronic era results in expectations that are not valid, cannot be fulfilled, and are not perceived realistically by individuals and even organizations.

There is a confused legal situation as well in the United States. Since electronic mail services, be they private, commercially offered by the traditional communication carriers or by independent vendors, utilize the common telecommunications network of the country, they fall under the jurisdiction of the United States Communications Act of 1934 while such mail is in electronic transit. Such electronic mail services also use computer systems owned perhaps by government, perhaps by an individual, or perhaps by a commercial company. Information in the custody of one of them might be subject to the Privacy Act of 1974, to other privacy law in the 50 states, to various telecommunications regulatory rulings, or even to no law. If a particular electronic mail service uses the United States Postal Service as its delivery means, and some do, then various postal statutes come into play.

What historically had been a conceptually simple situation has become a mishmash. So long as mail was the sole province of the Postal Service and involved the delivery of physical objects, legal protection could be assured. The Postal Service even had the authority to extend its obligations and responsibilities to contractors that might work for it. The arrangement though was the culmination of 300 years of evolution of a national mail system. What has been one postal service operating under a prescribed set of laws with delineated protections, all of which led to widespread public understanding and expectations about the system, has become a jumble of technological, legal, organizational, jurisdictional and not well-perceived fragments. For

example, a commercial vendor of electronic mail services has no authority whatsoever to compel telecommunications carriers to provide protection against electronic eavesdropping. In another instance, an administrative ruling originally created for telegraphic service has been applied to compel six months storage of electronic mailgrams.

Telephone Systems

Over the years, the United States has had one national telephone system whose implicit authority resulted in standardization of equipment, operational procedures, functional capabilities, and service. Foreign attachments to the system were prohibited, and various laws (the Wiretap Act, for example) and administrative rulings (for example, by state Public Utility Commissions) established details of protection for not only the conversations when en route through the telephone network but also for the billing records. Given the forced breakup of the AT&T, post-divestiture as it is called, many of the prior characteristics remain true but important differences have appeared. Among others, a very aggressive and innovative consumer electronics industry has produced a wide variety of devices that anyone can buy, attach, and use, subject only to prescribed technical rules by the Federal Communications Commission which regulates telecommunications.

The expectations of the past may or may not carry forward; and to the extent that they do not, individuals and even organizations are likely not to realize the change either in exposure of conversations to potential eavesdropping or in protection of billing/accounting records.

A technically obvious and recently publicized example of the abrupt shattering of historical expectations is that of the cordless telephone, ones whose handset communicates with the desktop part by radio. Since it uses radio transmissions, whose reception is well understood and for which appropriate equipment is readily available, the possibility of unauthorized access to conversations has increased sharply, and there are instances of interception of telephone calls with ordinary FM radio receivers by law enforcement authorities. No longer does the Wiretap Act seem applicable; its name is even wrong. In fact, the 1934 Communications Act would seemingly apply, but it allows reception of radio transmissions freely as long as the information gained is not

passed to a third party. No longer does a state Public Utilities Commission have total control of the telephony situation because the Federal Communications Commission at the national level is in charge of overseeing use of the electromagnetic spectrum.

An individual has developed an expectation of privacy for his voice conversations because he knows through media treatment and other sources about wiretaps and various laws to control them. He is very likely to extend that same expectation to data transmissions because he reasons that the same "telephone system" is used in either case, but the United States Wiretap Act specifically applies only to aural conversations. Largely unpublicized but equally interceptable are systems such as cellular telephones, mobile telephones, and the recently introduced AirFone in commercial aircraft.

PRIVACY ALERTING

Our discussion so far vividly illustrates how easily privacy issues can emerge or be latent and be completely unnoticed. Individuals might not notice; organizations, even a responsible one that originates some computer-based or communications system, might not notice. Government is the least likely to notice, and even less likely to take remedial or preventive steps unless a major cause celebre has developed. Thus there are major unresolved questions:

- Who is responsible for identifying and flagging new privacy issues?
- Who is responsible for alerting society?

There is no absolute answer to such questions, but I will note that the technologists initially were strong voices in the United States and still are. More recently, there are groups within the legal community that are actively supporting the general cause of privacy and, importantly, introducing privacy concerns into law curricula in significant ways. The issue is also being addressed in the legal professional societies, but in only a few places.

Information specialists and technologists clearly will have an ongoing role, largely because they will be most perceptive of the ways in which information can leak into unauthorized hands. Consumer groups will clearly play a role. Governments are not likely to play a role in the alerting process because democracies tend to be reactive. They address problems after they have arisen; normally they do not take preventive steps to deter a problem a priori.

SMALL VERSUS LARGE

Next, a closely related issue which I would like to call *privacy in the small* vs. *privacy in the large.* It revolves around the volume, or total amount, of some kind of information that can be related to an individual. It is easily illustrated in terms of the ubiquitous telephone number.

A lawyer will argue that an individual can have no expectation of privacy with regard to a telephone number because he is compelled to provide it in order to complete a call. In terms of the language in the Privacy Act of the United States, it would be called a routine use of a telephone number, as would many other things such as listing in the directory, doing statistical traffic analysis, and billing. In the small, one has to agree.

However, in the large, I would argue that the expectation is quite different because the totality of the numbers that one calls over time is very revealing of lifestyle, of one's friends, of the organizations that he does business with, of perhaps his travels, and possibly also of events. While the latter might not be illegal or criminal, they might nonetheless be ones that a person does not wish to have publicly visible; for example, social interactions with persons of like sex.

The expectation in the large would be that the so-called billing or accounting records should be protected against access by unauthorized parties. Indeed this is so because such records are generally protected either by law or by administrative ruling, especially against access by law enforcement authorities.

The point extends to many other categories of information, for example travel arrangements. One trip reveals little, generally, but a year's worth of trips and other reservations might be very valuable information in some circumstances.

NETWORKING

Let us try a different issue that arises from technology advances. At one point in time a computer-based information system served its specific population of users, and in fact most are still of that nature. Privacy concerns centered around the system, its set of users, the organization that owned the system, and the manner in which information was used. To the extent that sharing among systems occurred, it has generally been of small volume and by relatively slow means; for example, exchange of magnetic tapes.

Modern communications technology has made it possible for computers to communicate with one another on a second-by-second basis or to exchange large volumes of information through all-electrical connections. Networking, as it is called, is common within many systems already; for example, computers in the authorization system that supports bank credit cards automatically dial one another periodically to update records and even whole databases. But networking across systems which are not in the same company or even in the same community of companies is beginning, but is not yet commonplace. Let me clarify what I have in mind.

Many large corporations operate extensive networks for their internal affairs; I do not mean them. Many business communities operate networks that include a large number of corporations. The financial community is an obvious one. Banking is networked worldwide and the privacy concerns can be addressed collectively for the whole community, subject only to the details of transborder dataflows and the variation from country to country. I do not mean such community-of-interest networks.

I do mean situations such as the following example.

A Retail Example

It has become popular in the United States for large grocery markets--the supermarkets--to use automated checkout stands. The most recent ones scan special codes on merchandise with a laser device, and consult a database in the attached computer for price and other information. To the extent that such a device functions like a traditional cash register, it is not a problem. It calculates the bill and provides an itemized receipt. It may also do inventory control for the market, and it may automatically produce orders for restocking of merchandise, but such information is impersonal and not related to individuals by name.

However, it is popular in the United States to pay for groceries with a bank check, and there is a lot of concern about bad ones, those without funds behind them. A specialized industry has arisen to verify checks offered in payment not only for retail markets but anywhere. Basically such a system keeps track of individuals who pass bad checks, of delinquent accounts, and of account numbers that correspond to lost or stolen checks. Obviously, it is a system with positive social value. There is no question that such an automated scheme is a wise business approach, and there is no question that it is good for the consumer as well because the losses from bad checks will be passed on to the consumer in the price structure.

Thus, we find that the automated checkout stands have been electrically internetted to the automated check-verification systems. The latter serve a large number of retail outlets either by permanently connected or dial-up telephone connections. It is an instance in which a large number of organizations in one business community--the retail business--individually internet to a few systems in another business community that provide services nationwide.

Incidentally, note that a local retailer's system could, if he wished, also capture information about the individual. If the check verification system is to work, some identifier must be entered from the same keyboard that is used to ring up purchases; typically it is the number on one's driving license. The retailer can buy a mailing list from the Department of Motor Vehicles in his state, or he might opt to

enter the name and address directly since these data elements are commonly also on the check.

For those stores that accept bank cards, there can be a corresponding automated interface to the bank card authorization system. The debit card is coming into use in the United States, as it is also in Europe. Inevitably there will be an automated interface from checkout stands directly in one's bank.

Systems such as in this example which internet across functional lines, or across business communities, are the ones that I do have in mind.

Obviously we do not want to make laws that try to control information use in the retail market area. Even if we unwisely did, would the grocer or the retailer who connects his payment system to a check verification or debit card system, appreciate the privacy consequences? To him, it would be a sound business decision, not an informational privacy matter. Even if there were privacy restrictions governing retail records and even if he diligently obeyed them within his own establishment, would he think to ask what the "other system" to which he is connected might do with the information he forwards to it? Is he even in a technical position to notice the point? And even if he were, the business advantage would probably overwhelm any privacy considerations.

The salient point is that networking per se, even though in the best of business or other motivations, can inadvertently transgress on privacy protections. The risks can become significant because so much information about the individual is, or can be, aggregated in one place. We should also notice that networking can circumvent security protections that might be present in a system. To the extent that the business sector becomes extensively networked in the functional sense that I have noted, then the privacy problem becomes increasingly difficult to deal with under law; and the *system security* problem becomes more and more like the one faced by the military and defense establishments.

BYPRODUCT COLLECTION

Here is another broad aspect of the future. Much information about people will be collected as a byproduct of a transaction; the debit card is a good example. As an individual moves through his daily life, his bank will have been contacted many times to record a payment for some expenditure. At minimum, his pattern of spending will be captured in the bank records. The bank in its own interest and protection will more than likely time and date every transaction, not only for audit purposes but also to resolve errors. By combining such information with the names of the merchants from whom he has purchased, his physical whereabouts can be ascertained.

Let us suppose that banks aggressively move into new directions of business. Throughout the world, the telephone system is becoming heavily computerized. The mere presence of a large very capable computer, whose power can be extended far beyond simple telephony needs at modest marginal costs, will, and already has in the United States, lead the telephone companies to offer general data services to subscribers. Many banks, major ones at least, have large computer installations. Why should they not go into the business of offering general accounting services to smaller retail merchants? If a bank were to do so, the precise details of every purchase would also be in the bank computer records, in addition to what is already there. The details of an individual's life have become distressingly centralized on one set of records.

The exchange of information between the merchant and the bank is for the purpose of a payment transaction, a legitimate business motive. One cannot argue about capturing the information necessary to make the electronic funds transfer from payor to payee; nor can one argue that it must be retained for some period of calendar time to resolve possible errors and to provide for audit reviews. The risk comes when additional information gets into, or can be related to, the basic record; for example, information such as mailing addresses, or purchase records, if a bank happens to be in such a line of business.

APPROACHES TO PROTECTION

Let us pause for a moment with these last two aspects--internetting and byproduct collection--to try out some ideas for doing something about providing privacy in such an environment.

There will be no way that we can prohibit a retailer from connecting himself to other services, such as a check verification service; nor will we be able to prohibit a bank from getting into other lines of business. The United States is in an age of deregulation which means that a lot of historical prohibitions about how businesses work will vanish; and it already is beginning in banking. What could we do?

Legal

We might seek a law that provides an umbrella of protection over (say) retail customer records. If we were bolder, we might try for a law that extended the protection to other systems with which the retailer might interconnect. Or we might try to imagine reasonable interconnections of systems, based on probable business relationships, and try to address combinations of business records in law. The United States Privacy Protection Study Commission adopted this last view. It suggested, for example, that insurance companies plus their various supporting organizations be treated as a single entity for privacy purposes. Even if we were successful in doing this once or twice, we would soon find ourselves in a never-ending sequence of new laws as technology and business applications of it create a steady stream of new systems and interconnections.

Technical

We could ask a technologist how to address the problem. He would probably observe that the basic amount of information necessary to conduct the essential transaction would have to be collected and that's that. It would be analogous to the single telephone number; the expectation of privacy for the minimum data necessary to complete the transaction would be nil. But he would also observe that we ought to install good computer security safeguards in order to protect even the minimum data relevant to each transaction against unauthorized access;

and we ought to make sure that authorized users of the information are identified in automated audit trails and be governed by strict security-oriented procedures and management oversight. In short, he would advise us to do the computer security job comprehensively and properly.

On reflection, he would probably notice another thing. He would observe that the privacy risk escalates if we allow collateral information not necessary for the basic transaction to be blended, accidentally or intentionally, into the records. Pursuing such an idea, he might suggest to us that mailing addresses be kept completely separate from the financial transaction information and never allowed to mix with it. Somewhere deep within a computer would be a carefully protected table that would link financial data to mailing information solely for the purpose of preparing billing statements. Such a table would have extensive error controls to assure that wrong data elements could not be linked; and access to it for the purpose of updating would be carefully limited to a few trusted persons.

Going one step further, he might propose that all records be treated in the spirit of the anonymous Swiss bank account. Wherever data might exist that could create a potential privacy risk, all identifiers associated with the data would be anonymous. Sooner or later, though, data would have to be aggregated for collateral purposes such as mailing of statements; but in every such instance, the system would consult its carefully controlled tables to aggregate anonymously identified data elements for legitimate business needs.

His line of argument would be that privacy protection would be assured by means of a very elegant set of technical security safeguards which will assure that all sensitive information has only anonymous system-assigned identifiers, and that all relationships among such data will be governed by carefully controlled and protected tables to which only trusted individuals will have access. Correspondingly, the software processes that would work with such tables to aggregate anonymous data elements into complete records will similarly be carefully designed, checked, maintained, and controlled by trusted individuals. In fact, the anonymity might start even with the collection of data incident to a transaction. An individual might carry one of the so-called "smart cards" whose internal electronics can

transmit in encrypted form the anonymous identifier that only the internal protected tables can associate with a specific individual.

Such a suggestion has merit because it effectively centralizes all the potentially trouble-making software processes and the control of access to sensitive data in a set of tables and some associated software. It would be quite unlike today's systems which generally put all manner of data together in one set of records--the popular integrated data base--and generally distribute the security problem throughout the system, especially throughout all manner of software.

But there is a very serious other side. In the name of privacy we would attempt to dictate the general architecture of systems that process sensitive data. I do not know how one would write such a law, nor do I know how one would oversee its enforcement.

FILE MATCHING

Let us come back to the central theme and press onward, but this time we will give the example first and identify the issue afterward.

It has become popular in the United States to match computer files from different agencies in an effort to identify individuals that in some way are in defiance of the law. For example, tax information files can reveal whether an individual earns too much income to qualify for public welfare assistance. In each case, the files of interest are ones that were collected for some quite specific purpose but the routine use provision of United States law did not include matching with unrelated files. In each case the underlying payoff to society was deemed positive and not in question. As one might anticipate, the results from early attempts were very much in question; and there were many indviduals improperly accused of wrongful actions. Guidelines were developed within the government for the conduct of matches by its agencies, and more recent attempts have been more palatable, although the economic return from the effort has often been questioned as being far too small to have justified the privacy exposure or potential harm to individuals.

Whatever one may think about the desirability of computer matching, it does raise an interesting privacy issue. Files from different sources are very likely not to be consistent with regard to individual

identification. Names will have been spelled differently; addresses may have changed; errors may have occurred. At least in the United States, there is no universal personal identifier that makes matching a certainty. Hence, in the "hit list" resulting from matching two files there will inevitably be many individuals who are present only because the computer process could only guess that records in the two files pertained to the same person. Later, manual processing will resolve the ambiguity and clear the innocent; but for a time at least, one can be under suspicion not because of a reasonable expectation of a wrong having been committed, but because of "noisy" computer data and the software matching processes that try to deal with it. We are not talking, of course, about the legitimate hits from the match; such individuals have in fact crossed the law and deserve the consequences.

Such an approach is certainly inconsistent with the usual legal attitude that would be much more careful about making even an implied accusation without decent evidence of wrongdoing. From a privacy point of view, there has been an invasion of privacy for some people on the hit list even though there has not been any subsequent negative or harmful action. Is this a privacy dimension that we must be concerned with? Perhaps not in the computer matching process as it is now practiced, but suppose that one's mere presence on a hit list is retained and used later for other purposes; suppose it becomes the basis of what lawyers call "fishing" through facts in the expectation of finding something wrong. Combine "invasion of privacy without action" with the earlier comments about internetting of systems, and one may have a very important issue a decade or so from now.

OFFICE AUTOMATION

Let us think about the office environment and its automation, combined with the expectation issue raised earlier. It will raise a rather different connotation of privacy.

In the traditional office of personal desks, file cabinets, and their contents, there is an expectation of private ownership. It extends especially to the contents of one's desk and to lesser things such as the contents of a rolodex or mailing list. An individual will often feel uneasy entering another's desk even though the relationship

between the two may be a well-established one between an individual and his secretary or colleague. It is almost as though the established tradition of the sanctity of a personal home and belongings has been extended to one's workplace; one does not enter without having been invited.

Whether it is a feeling of personal turfdom as with a home or the fact that one has himself created the letters and memos in files, whether it is an emotional question or even biologically based, it is clear that such expectations of privacy against physical invasion of things which are regarded as personally owned exist and are strong. It is not clear that they are well founded or even essential, nor is it clear whether such expectations will pass over time; but in an automated office environment, ownership of things--notably on-line files--is likely to be shared.

Ownership

There is also the question of who owns information stored in a computer. United States law has held that the organization owning the computer also owns its contents. Such a position is quite inconsistent with the normal view that the contents of one's desk are generally not open to prying by corporate eyes. The same question of ownership becomes exceedingly important in the case of electronic mail systems, especially if the system provides such mail services to the general public. There has already been a major incident with regard to a government-owned computer and the electronic mail in it.

One would anticipate that such an expectation of *ownership privacy* would be important for the ready acceptance of office automation systems and their electronic mail features by an organization. It would seem a good principle that office systems should generally meet the same expectations of the paper office, or at minimum, not drastically offend the a priori expectations based on decades of being embedded in a traditional office.

PRIVACY AND SECURITY

It is time now to relate such privacy issues to computer security. Privacy of course relates generally to information about people and how it is used. It may be used to deny access to some entitlement or privilege; it can be used to seriously harm, such as destroying an individual's credit status. It can be used to annoy as with unwanted mailings or solicitations that depend on information lists obtained from records collected for other purposes. It can relate to ownership of information and one's personal feelings about such ownership.

In whatever dimension though, if information is to be used for legally or socially accepted purposes and not for spurious purposes, it must be protected against loss, modification, or theft, and access to it must be controlled. In the last aspect, "access" could be by individuals or it could be by another computer-based system. Safeguards for such protection and for access control are collectively the body of knowledge that we generally call "computer security." Clearly, if privacy protection is to be provided with high confidence, computer security safeguards must be in place first.

I would not pretend for a moment that our systems today are well-off from the view of computer security, but at least the principles of doing the job are rather well understood. There is a growing body of expertise that can deal with it, and significant research is under way on many of the technical parts. We have come to understand that comprehensive computer security will require attention to physical protections, hardware safeguards, software safeguards, safeguards for communication, personnel control, proper procedures, and attentive management oversight. There are ways to do risk assessment, and to decide what safeguards are appropriate. For the organization that wants to install security safeguards and that is willing to make the necessary investment, we do know how to install system-wide safeguards for many kinds of installations. In particular, we know how to do the computer security job for a system that involves one or a connected set of processing centers and serves a user population indigenous to the system, and that is under a common--or at least coordinated--management structure. We even know how to take care of a cohesive community that

is willing to work together. The financial community is such an example.

When we introduce internetting, the situation is much less promising. Especially will it be troublesome if the systems were not intended originally to communicate, or if the systems are to share only specified parts of records with one another. Especially will it be troublesome if the systems are under unrelated managements, or parts of different federal agencies or corporations, or under the regulatory purview of different laws. Quite aside from the managerial or legal aspects, or the distribution of liability among internetted systems, or of even knowing whether all systems are complying with desired privacy and security guidelines, there are major unsolved technical problems related to providing *network-wide security* safeguards.

LEGAL FRAMEWORK

Let us look now at the legal part of the matter. For an information environment that

- will be extensively internetted,
- will collect much information about people as a byproduct of other transactions,
- will abruptly and perhaps invisibly negate expectations of privacy and ownership as technological advances are made, or
- can induce differing expectations depending upon "small vs. large," and
- may incur invasions of privacy without subsequent immediate action,

what legal framework can we imagine that will embrace a future of such diverse and complex structure? What philosophical legal approach will accommodate a future of the kind we anticipate?

Traditionally, privacy law in the United States has given the individual the right to compel proper behavior of an agency, and it has been targeted on a specific body of records. He can require the correction of a record, and the dissemination of the correction to all

who received the erroneous record; he can require the deletion of some information; he can compel an agency to abide by its "routine use" public position. Beyond that, the individual has no standing for action. Can we adopt such an approach in trying to deal with the privacy problems of the future? Can a "code of fair information practices" be conceived and implemented in a law that will span all the aspects of privacy concerns that we can foresee? Will a "targeted approach" ever be able to keep up with the problem?

Traditionally, Europe has adopted what I shall call "positive control." A Data Protection Board or an equivalent organization monitors record-keeping organizations for compliance with law, and plays a very definite proactive role in establishing the conduct of the record keepers. Can such a regulatory body be extrapolated to deal with our projected future? Could it possibly attempt to license beforehand all the possible informational linkages that business, industry, and government might conceive? Would it even be acceptable for such a Board to intrude itself so deeply into nongovernmental affairs in the private sector? Might not the problem be so huge that it would overwhelm even the best-intentioned positive control effort?

A third possibility is that we tell the individual that it is all his problem. We could take the position that the formal institutions of government cannot help because the future is too complicated, and that we cannot design appropriate law that will afford privacy protection but at the same time not be intrusive and excessively binding on the conduct of a country's affairs. If we go such a way, how do we assure that individuals are well enough informed to be alert to problems and to know what legal remedies are available?

As another option, can we conceive an umbrella approach in which one law is meant to apply to many and diverse organizations that deal with information about people? Or do we use an area-specific approach, as the United States has? The latter has a separate and different law for credit, for education, for federal agencies at large, for census data, and for tax information. The European approach approximates an umbrella aproach; the United States, a targeted approach. Incidentally, the latter is likely to stay that way simply because of the difficulty in establishing a constituency for broadly based action.

Or we could try some combination of them, plus others that have yet to be innovated. To date, we all have drifted forward--the United States on its approach and Europe on its. We have not had a significant dialogue on the underlying question of which, if either, is appropriate for the future. We probably need to inaugurate such a public debate promptly.

Information Representation

However we decide the general legal approach and however we design the laws, there is an important trap to avoid; it has to do with the information representation issue that has troubled the protection of things under copyright. Whatever personal information we decide to legally protect must be assured of its protection whether it is stored in a computer, written on a magnetic tape, in transit over a communications channel, or printed on paper; and it must be so internationally. As far as I know, privacy law has not stumbled in this regard, but it could happen. For example, some years ago the United States Congress created a wiretap law which applies only to aural information. It has not been illegal so far to intercept data communications, but any technical specialist will tell you that one cannot decide from looking at a stream of digital information whether it is a data communication or a voice conversation that happens to be represented in digitized form. We will have to be cautious in the design of law to avoid creating circumstances readily circumvented by technology. So to speak, the protection embodied in the law will have to be indifferent to technology.

THE WORLD AHEAD

Where does that leave us, as we look toward the future and try to imagine what new privacy issues will emerge and how we will deal with them? First, note that information is a very universal commodity; all organizations and all people must use it to achieve purposeful behavior. Therefore, the world will increasingly be stiched together more and more intimately by its information threads. Technically, this will mean extensive data communications and internetting of systems. Databases

will not be confined to textual information; they can also include audio and video that can be searched, combined, or displayed as readily as text and perhaps combined with it. Internationally it means continuing attention to transborder data flow issues. For each company it will mean ongoing and increased attention not only to computer but also to system and network security safeguards.

The privacy and security problems that will arise are likely to be basically the same for all countries that have about the same stage of technological advancement. The developing countries will encounter the problems later on; but on the other hand, technology exporting countries will drive the issue, and the developing countries may see the problems much sooner than might be anticipated. International business communities (for example, banking) will tend to spread any privacy or security problem worldwide but such communities will also be very important focal points for achieving action.

Solutions though are likely to be country dependent. Many years ago Dr. Claes-Goran Kallner, the first chairman of Sweden's Data Privacy Board, cautioned me that privacy solutions that might work for Sweden would not necessarily work for the United States, simply because of the difference in geographical size. I was not to appreciate his observation about the importance of scale factor until my understanding of the privacy issue in the United States matured some years later. Size does make a difference.

Solutions will also be country dependent because of cultural heritages. European countries are accustomed to population registers, to personal identifiers, and to federal-level record-keeping procedures over the population. The United States is very resistant to all such federal intrusions into the life of the individual.

Technical Issues

There are new and tough technical problems before us. For example, if it were to prove desirable to legally constrain the kinds of information--or even specific data elements--that could be electrically exchanged among systems, we have technical problems in the commercial world that have been faced only in the military and defense world. If we became convinced that the only way to handle commingled sensitive

data in a system would be to keep it anonymous in the file but aggregate it with high-confidence software processes, we have a whole new dimension of computer security for which we would need not only new technical solutions, but also ways in which to specify to vendors and to systems implementers how their hardware and software should function. In a sense, we would have imposed a very new and quite different functional requirement, even architectural requirement, on vendors in behalf of privacy.

In that regard though, the complaint would be one of "too expensive"; the position would be that "we cannot afford the computing power to implement such an involved scheme." To such a position I hold a personal view that I think is pertinent. The cost of computing power has been declining dramatically for decades; we have exploited it to enhance the level of automation in the information infrastructure that supports our countries, societies, and governments. We must now be equally diligent in using computer power to assure ourselves that a creeping information-intrusiveness does not occur.

Personal Impact

The evermore extensive record keeping and the drive for automation in behalf of efficiency and economic operation throughout all parts of society and a country are gradually tightening the processes of society. We do not enjoy options that were available to individuals only a few decades ago. It is virtually impossible to be personally anonymous without forsaking the standard of living and privileges of a our modern world; one would have to withdraw completely from society. Even our personal money management is impacted; not only is the money float in our personal accounts gradually diminishing but banks decline to make funds available until several days after deposit. In the extensive information infrastructure that modern countries and society must have to function, we cannot allow the analog of environmental pollution to develop.

We must concern ourselves in an ongoing basis with the use of information and its protection. But what about the individual? Where will he stand? In the end, it is he that privacy really concerns, and it is he that loses if we, who are the attentive professionals in this area, are careless or irresponsible.

PRIVACY LAW AHEAD

As I look toward the future of not only countries but also a world of highly internetted information systems, each complex in itself, but which transcend national borders, federal agencies, governments, corporate boundaries, and boundaries of business communities, I cannot imagine a single legal construct that can accommodate the situation. Laws of today that were constructed for monolithic situations will not be satisfactory for systems and combinations of systems that transcend jurisdictional boundaries.

For those bodies of information that are now covered by extant law, we should let well enough alone other than to plug loopholes and revise the protections. Whether we have achieved the law with a targeted approach or an umbrella approach really does not matter, so long as the transborder question can be handled. There will be some new bodies of information about people that will deserve a specific law; for example, electronic mail is presently under consideration in the United States. There will be some business communities that can be treated as a single entity.

But what about all those other circumstances and situations? What about all the opportunities for connecting systems together and for exchanging information about people for whatever purpose, but which might never put a large enough group of people at risk to get federal or even state attention? What about expectations--the reality of present socially accepted systems vs. the consequences of technological advances? Or expectations in the small vs. in the large?

PERSONAL RESPONSIBILITY

My view is coming to be that there will be a large part of the privacy issue for which the individual will have to take care of himself. Major parts can be handled by law as they are identified, but the individual will have to be on his own for a lot of things. That may be fine, but he will need a basis for remedial action when necessary. One approach might be a form of insurance, perhaps required of all businesses just as are business licenses. It could even be insurance at the federal level, just as a United States agency now insures savings

account deposits. Alternatively, we could provide the individual with a legal basis for remedy. For example, we could give him standing to bring civil suit and recover damages. Such a course is a little tricky because it might be hard to show damages related to information misuse. If that is a viable possibility, hopefully legislators can design appropriate law. However, let us not overlook the international aspect in an era of internetting. It will be perfectly possible for the misuse of information to occur in a country other than one's residence or other than the one in which he happens to be at the moment. We will have the problem of harmonizing privacy protections worldwide.

If he is to take care of himself, the individual will also need to be well informed about information matters, because many things that might concern him will probably not be particularly visible. I have no insightful suggestions beyond the usual ones--consumer protection groups, government publications, activist information professionals everywhere, appropriate educational content throughout curricula at all levels, and certainly proper content in the curricula for technical people so that they understand how to build the right kind of systems and can also conceive new technical ideas.

On balance though, it would appear that a combination of approaches can make a very livable world from the information privacy point of view. It does not look hopeless to me; there are ideas. It may not be easy, but there are several principles that can be helpful. Moreover, we have not really begun to think about privacy in the very broad perspective that I suggested this morning. How to get there from here though is quite a different matter, and a topic for another occasion.